Tento projekt je spolufinancován se státní podporou Technologické agentury ČR v rámci Programu Národní Centra kompetence.
www.tacr.cz
Výzkum užitečný pro společnost.

Výsledek výzkumu a vývoje projektu TN01000024

Identifikační číslo: TN01000024/21-V1

Název: Metodika návrhu síťového prostředí (Methodology of Network environment design)

Abstrakt: Svět bezpečnosti provozních technologií (OT) průmyslových řídicích systémů (ICS) je nucen neustále reagovat na výzvy a hrozby, na které, ještě v nedávné době nebylo nutné, s ohledem na odlišnosti od běžných IT systémů v organizaci, aktivně reagovat. Incidenty, jako byly ransomwarové útoky na společnost Colonial Pipeline a JBS Foods, poukazují na komplexní prostředí hrozeb, kterým tyto systémy čelí.

Tradiční kybernetické útoky na IT se zaměřují na boxy Windows/Unix like systémů využívající zero days (dříve neznámé zranitelnosti) zranitelností nebo jejich nebo dalších slabiny s cílem narušení dat (získání, modifikace, odepření). Ve velké části zneužívají neznalosti/nepozornosti koncových uživatelů, kteří s těmito systémy pracují. Více než na sofistikované útoky typu APT je IT bezpečnost více zaměřena na odhalování vnitřních tradičních hrozeb.

Autoři: Burčík J.

Typ výsledku: O – ostatní

Termín dosažení: prosinec 2021

Umístění: České vysoké učení technické v Praze, Jugoslávských partyzánů 1580/3, Praha

Tento výsledek byl vytvořen se státní podporou Technologické agentury ČR v rámci programu Národní Centra kompetence, projekt č. TN01000024, Národní Centrum Kompetence-Kybernetika a umělá inteligence (NCK KUI).

Metodologie návrhu síťového prostředí

Methodology of Network environment design

(pro zajištění kybernetické bezpečnosti průmyslových řídících systémů)

Jaroslav Burčík, ČVUT FEL, burcik@fel.cvut.cz

Úvod

Svět bezpečnosti provozních technologií (OT) průmyslových řídicích systémů (ICS) je nucen neustále reagovat na výzvy a hrozby na které, ještě v nedávné době nebylo nutné, s ohledem na odlišnosti od běžných IT systémů v organizaci, aktivně reagovat.

Incidenty, jako byly ransomwarové útoky na společnost Colonial Pipeline a JBS Foods, poukazují na komplexní prostředí hrozeb, kterým tyto systémy čelí.

Tradiční kybernetické útoky na IT se zaměřují na boxy Windows/Unix like systémů využívající zero days (dříve neznámé zranitelnosti) zranitelností nebo jejich nebo dalších slabiny s cílem narušení dat (získání, modifikace, odepření). Ve velké části zneužívají neznalosti/nepozornosti koncových uživatelů, kteří s těmito systémy pracují. Více než na sofistikované útoky typu APT je IT bezpečnost více zaměřena na odhalování vnitřních tradičních hrozeb.

Profesionální kybernetický útočník přistupuje k útoku na ICS systémy komplexně, identifikuje fyzická zranitelná místa řídicích jednotek, procesů a hledá způsoby, jak tato zranitelná místa využít pomocí digitálních manipulací. Oproti běžným IT útokům je v této oblasti od útočníka stále vyžadována vysoká odborná znalost řízeného fyzikálního procesu a domény řídicího systému s jeho jedinečnými konstrukčními vlastnostmi, proto aby dokázal nalézt a zneužít její zranitelnosti. Útoky typu Stuxnet využívaly specifických vlastností architektury návrhu ICS systému, který není z principu možné opravit instalací bezpečnostní záplaty.

Pro úspěšný sofistikovaný útok na ICS systém je nutno týmové práce specialistů na IT, lidí ovládající vlastní řízení fyzikálního procesu, případně specialistů se znalosti fungování dodavatelského řetězce. Je zřejmé že obdobným způsobem by se pak obdobně mělo přistupovat i ke složení týmů, které namýšlejí systémovou obranu.

Aktuální situace

Pokud máme řešit problematiku kybernetické bezpečnosti OT/ICS systémů, je nutné charakterizovat, jak takový systém vypadá a na jaké úrovně analýzy se pohybujeme. Srozumitelnou a vysoce

vypovídající studii ukazující problematiku útoků s vazbou mezi IT a OT/ICS systémy je možné nalézt např. zde [1]

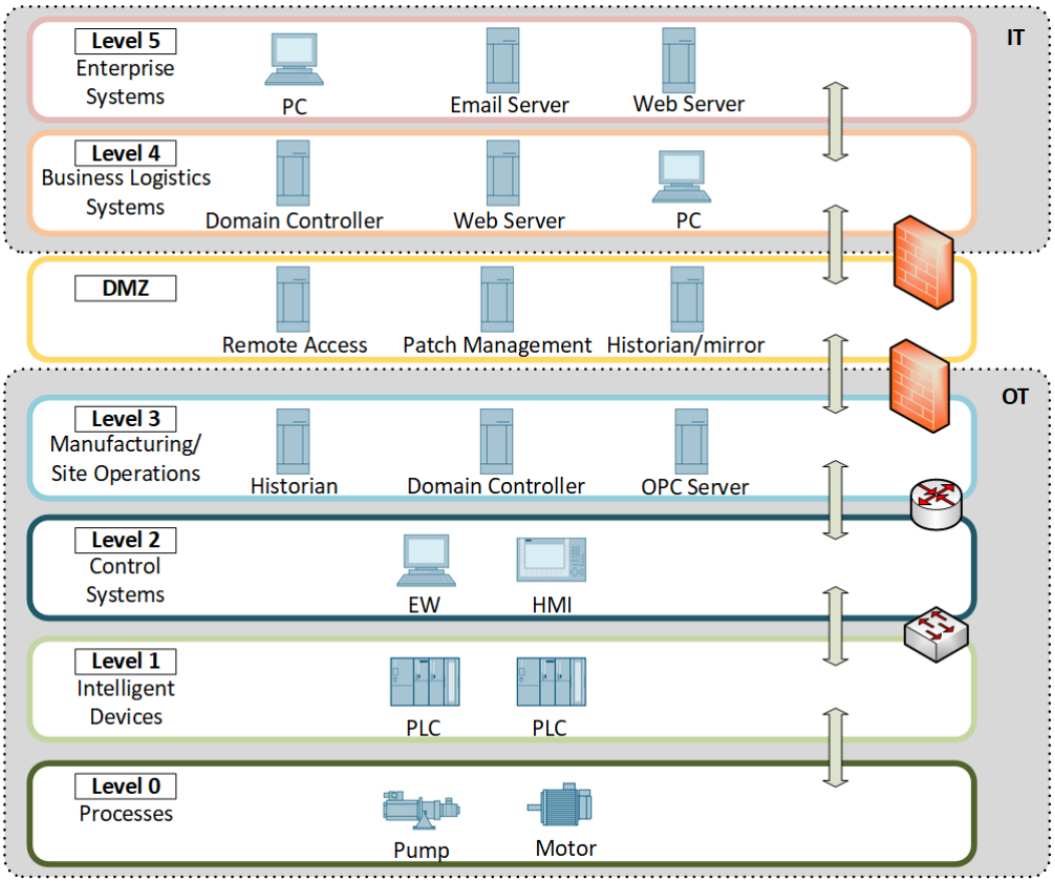

Figure 1 An adaptation of the Purdue Enterprise Reference Architecture by ISA-95 from G. M. Makrakis, C. Kolias, G. Kambourakis, C. Rieger and J. Benjamin, "Industrial and Critical Infrastructure Security

Kde jednotlivé úrovně vyjadřují toto:

- **Úroveň 0** - Senzory motory, čerpadla a ventily, tj. přístroje, jejichž hlavním účelem je poskytovat systému snímací nebo ovládací funkce přímo vztažené k fyzikálním veličinám či procesům
- **Úroveň 1** - Inteligentní zařízení, která snímají, monitorují a řídí fyzikální procesy. Jako jsou programovatelné logické automaty (PLC), PID regulátory (PID) apod.
- **Úroveň 2** - Řídicí systémy používané pro dohled a monitorování fyzikálních procesů. Tato úroveň zahrnuje mimo jiné rozhraní člověk-stroj (HMI) a inženýrské pracovní stanice (EW)
- **Úroveň 3** - Výrobní systémy/systémy pro provoz na místě používané k řízení výrobního procesu pro řízení celého závodu např. OPC servery pro zajištění jednotného komunikačního rozhraní
- **Průmyslová demilitarizovaná zóna (DMZ**) - Vytvořena za účelem zabránění přímé komunikace mezi IT a OT prostředím instalací "zprostředkovatelských" služeb. Historicky tato DMZ neexistovala a ICS systémy se fyzicky oddělovaly od IT technologii. To však již dnes není možné. Nachází se zde různé proxy servery, servery pro vzdálený přístup atp.

[1] G. M. Makrakis, C. Kolias, G. Kambourakis, C. Rieger and J. Benjamin, "Industrial and Critical Infrastructure Security: Technical Analysis of Real-Life Security Incidents," in *IEEE Access*, vol. 9, pp. 165295-165325, 2021, doi: 10.1109/ACCESS.2021.3133348.

- **Úroveň 4** - Systémy pro podporu obchodu/plánování/podpory výroby. Patří se různé aplikační servery, e-mailoví servery a systémy plánování podnikových zdrojů (ERP).
- **Úroveň 5** – Další systémy na vyšší úrovni Enterprise architektury (korporátní síťová infrastruktura, systémy přístupu v rámci subdodavatelského řetězce apod.)

Ve výše zmíněná studie pak přehledně popisuje vektor útoku a ukazuje na jakou úroveň byl útok primárně veden (Obr2) a s jakou taxonomií (Obr3).

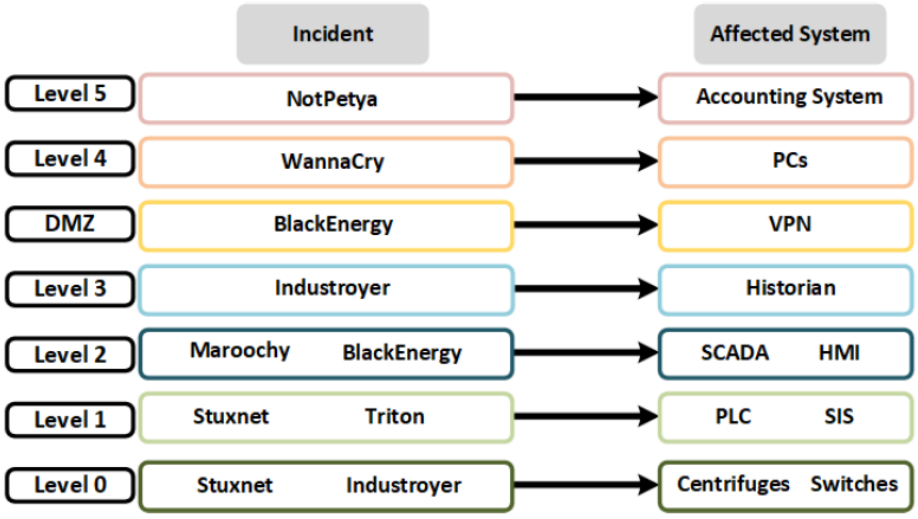

Figure 2 Correspondence of incidents to affected systems from G. M. Makrakis, C. Kolias, G. Kambourakis, C. Rieger and J. Benjamin, "Industrial and Critical Infrastructure Security

	Type 0	Type 1	Type 2	Type 3	Type 4
Stuxnet ([24])	●	●			
Duqu ([28])	●				●
Shamoon ([31])				●	●
Havex ([40])			●	●	●
BlackEnergy ([45])				●	●
Industroyer ([56])	●		●	●	●
Triton ([61])	●		●	●	
VPNFilter ([68])		●	●		
WannyCry ([73])		●	●		
Colonial ([89])				●	●
NotPetya ([81])		●	●	●	
Steel Mill ([94])					●
Maroochy ([96])			●	●	
NY Dam ([97])				●	
“Kemuri” ([101])		●		●	●
Slammer ([103])		●		●	

† Type 0: zero-day vulnerabilities, Type 1: known vulnerabilities, Type 2: insecure protocols, Type 3 : insecure configuration, Type 4: social engineering

Figure 3Taxonomy of incidents based on the types vulnerabilities from G. M. Makrakis, C. Kolias, G. Kambourakis, C. Rieger and J. Benjamin, "Industrial and Critical Infrastructure Security

Omezení dopadů takovýchto útoků však i skrze relativně velkou škálu různých frameworků které dnes existují pro řízení kybernetické bezpečnosti však není triviální. Pokud bychom měli identifikovat pro další práci ty nejvýznamnější, tak v této oblasti k nim patří:

1) The cybersecurity framework (CSF) - vyvinut Národním institutem pro standardy a technologie USA (NIST). Poskytuje podrobný soubor bezpečnostních opatření, které se zaměřují na vytváření jednotlivých profilů provozovatelů. Bezpečnostní opatření CSF jsou rozděleny do 5 oblastí: Identifikace; Ochrana; Odhalení; Reakce; Obnova.
2) ISO/IEC 21827 - zachycuje postupy, které se v průmyslu obecně používají. Model je standardní metrikou pro postupy řízení bezpečnosti zahrnující:
    a. celý životní cyklus, včetně vývoje, provozu, údržby a vyřazení z provozu
    b. celou organizaci, včetně řídících, organizačních a inženýrských činností
    c. souběžné interakce s dalšími odvětvími a interakce s jinými organizacemi (akvizice, řízení systému certifikace, akreditace a hodnocení).
3) ISA IEC ISA/IEC – sada doporučení která byla vytvořeny s cílem řešit otázky bezpečnosti specifické pro průmyslové a řídicí systémy (ICS) a provozní technologie (OT).
4) C2M2 – vyvinut americkým ministerstvem energetiky (DOE), aby umožnil organizaci vyhodnotit vyspělost kybernetické bezpečnosti jejích systémů. Bezpečnostní opatření C2M2 jsou seskupeny do 10 domén: Řízení rizik; Řízení aktiv, změn a konfigurace; Řízení identit a přístupu; Řízení hrozeb a zranitelností; Situační povědomí; Sdílení informací a komunikace; Reakce na události a incidenty, Kontinuita provozu; Řízení dodavatelského řetězce a externích závislostí; Řízení pracovních sil; Řízení programu kybernetické bezpečnosti.
5) ISO IEC 270xx – sada mezinárodních doporučení pro řízení informační bezpečnosti pro oblast IT systému
6) The global cybersecurity index (GCI) vyvinutý Mezinárodní telekomunikační unií (ITU), který hodnotí země podle jejich úsilí v oblasti kybernetické bezpečnosti. Hlavními oblastmi GCI jsou právní opatření; technická opatření; organizační opatření; budování kapacit; spolupráce.
7) The Control Objectives for Information and Related Technology (COBIT) - vyvinutý Asociací pro audit a kontrolu informačních systémů (ISACA) k provádění správy a řízení informačních technologií. Tento model má 5 úrovní vyspělosti, přičemž řízení je rozděleno do 4 oblastí: Plánování a organizace; Poskytování a podpora; Pořizování a implementace; Monitorování a vyhodnocování.
8) The systems security engineering capability maturity model (SSE-CMM) vyvinutý americkou Národní bezpečnostní agenturou (NSA), který má 5 úrovní vyspělosti určených k hodnocení/hodnocení bezpečnostních postupů na úrovni systémů.

Jak se ukazuje, žádný z těchto frameworku není zcela vhodný pro systémy ICS. Velká většina z nich postrádá doporučení pro zajištění odpovídající kybernetické bezpečnosti na úrovni 0a1 tzn. úrovni akčních členů, senzorů, pohonů atp. Jde zejména o sledování anomálií v jejich chování (např. změny měřených veličin postrádající vazbu na fyzikální systém

Velice pěkná přednáška následovaná diskuzí k tématu nedostatků stávajících metrik a metodik proběhla v rámci IEEE Tech Talk SCADA Control Systems 2021 dostupné zde[2]. Důležitá zjištění s diskuze byla tato:

1. Systémy řízení ICS jsou úzce provázány s řízením fyzikálních procesů, avšak hodnocení rizik a dopadů nebere ohled na možné škody vyplývající z ignorování chování řízených fyzikálních veličin (fyzika se ignoruje).
2. Neexistující nebo jsou popsány velmi omezené postupy pro forenzní analýzu IC systému
3. S ohledem na jinou skladbu požadavků na znalosti zaměstnanců OT/ICS systémů chybí odpovídající školení z oblasti řízení kybernetické bezpečnosti

[2] IEEE Tech Talk SCADA Control Systems https://www.youtube.com/watch?v=eZqkCC6wqcE

4. Účastníci semináře se shodli, že ačkoli se v oblasti kybernetické bezpečnosti ICS systému trh dynamicky rozvíjí, adopce moderních přístupů a technologií je pomalá a Kybernetická bezpečnost řídicích systémů je zhruba 5-10 let pozadu za kybernetickou bezpečností systémů IT
5. Rovněž panuje jistá kulturní bariéra mezi specialisty IT a OT prostředí a snaha podřídit OT oddělení pod IT přirozeně naráží jednak z důvodů různých cílů a zaměření těchto oddělení a nemalou mírou také s ohledem na obavy pracovníků OT ze ztráty pozic či zaměstnání.

Jak dobře shrnuje studie[3] stávající nástroje pro hodnocení zranitelnosti v oblasti kybernetické bezpečnosti byly navrženy na základě zásad a standardů definovaných organizacemi, jako je americké ministerstvo energetiky (DOE) a Národní institut pro standardy a technologie (NIST) či mezinárodní doporučení vycházejících z norem ISO 27000. Často se používají se frameworky jako je model vyspělosti kybernetické bezpečnosti (C2M2) či NIST Cybersecurity Framework (CSF).

Tyto rámce jsou výborné při provádění kvalitativní analýzy kybernetické bezpečnosti a identifikaci zranitelností, avšak neposkytují prostředky či postupy pro zmírňování zranitelností s cílem dosáhnout požadované kybernetické bezpečnostní vyspělosti. Ve výše zmiňované studii pak autoři představují framework který pojmenovali CyFEr - Cybersecurity vVulnerability mitigation Framework through Empirical paRadigm. Novost navrhovaného rámce spočívá v jeho schopnosti kombinovat techniky kvantitativního hodnocení se strukturami závislostí, aby bylo možné provádět rozšířené zmírňování zranitelností podle priorita navrhovaný rámec lze použít na úrovni aplikace, fyzikálního systému nebo organizace a řízení.

Autoři nového frameworku rovněž řešili jeho provázanost a orchestraci na stávající existující frameworky. Toto je velmi důležité při sbližování IT systém s OT/ICS systémy a jejich efektivní integrace v rámci Enterprise architecture[4]. V práci je dobře popsán stávající vztah mezi nově prezentovaným frameworkem a různými modely vyzrálosti kybernetické bezpečnosti.

Problémy, které dlouhodobě přetrvávají

Ačkoli na poli akademickém se vymýšlejí stále sofistikovanější přístupy a metody pro efektivní řízení kybernetické bezpečnosti v praxi panuje značně odlišná situace a systémy ICS trpí značným konzervatismem při adaptaci nových postupů a technologií.

SANS Institute[5], která je respektovanou privátní společností z USA zaměřující se na informační a kybernetickou realizovala v r.2021 studii která analyzovala 480 odpovědí napříč různými odvětvími od specialistů, jejichž primární odpovědností je důraz na ICS. Mezi nejzávažnější zjištění patřila tato:

- Připojení k vnějším k systémům zůstává i nadále převažující příčinou incidentů
- Organizace stále nedodržují osvědčené postupy segmentace sítě
- Téměř 20 % respondentů uvádí jako počáteční vektorů útoku využití technické pracovní stanice

[3] Sri Nikhil Gupta Gourisetti, Michael Mylrea, Hirak Patangia, Cybersecurity vulnerability mitigation framework through empirical paradigm: Enhanced prioritized gap analysis, Future Generation Computer Systems, Volume 105, 2020, Pages 410-431, ISSN 0167-739X,
[4] ISO/IEC/IEEE 42010:2011 Systems and software engineering – Architecture description
[5] SANS 2021 Survey: OT/ICS Cybersecurity, Mark Bristow, August 24, 2021 at https://www.sans.org/white-papers/SANS-2021-Survey-OTICS-Cybersecurity/

- Existuje jen velmi malá míra systémů které dokáží provádět korelace mezi analýzou procesních dat, chováním systému a výskytu anomálií, která mohou indikovat bezpečnostní incidenty
- Soupisy aktiv jsou pro většinu organizací stále problémem, pouze 58,2 % z nich má formální proces
- Slabinou se rovněž ukazuje nevhodně podchycené řízení dodavatelů a nedostatečné ošetření technologií pro vzdálený přístup.

Jaké bylo zastoupení jednotlivých útoků dle respondentů je možné vidět na obrázku 4.

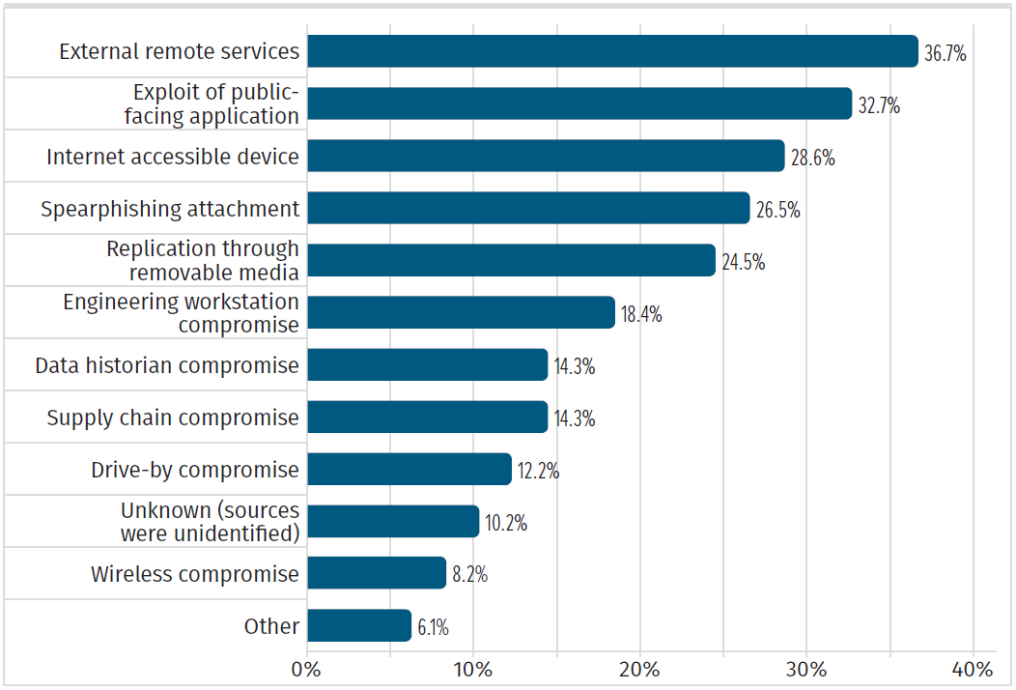

Figure 4 Initial attack vectors involved in OT/ICS systems incidents from SANS 2021 Survey: OT/ICS Cybersecurity

Dosti tristním zjištěním pak byla odpověď na otázku, jaké procesy používáte k odhalování zranitelností softwaru nebo hardwaru? Na obrázku 5 je vidět že v odpovědích převládá spíše pasivní či maximálně „best effrod“ přístup více než využívání nějakých sofistikovaných procesů či nástrojů, které jsou dnes běžné v IT prostředí.

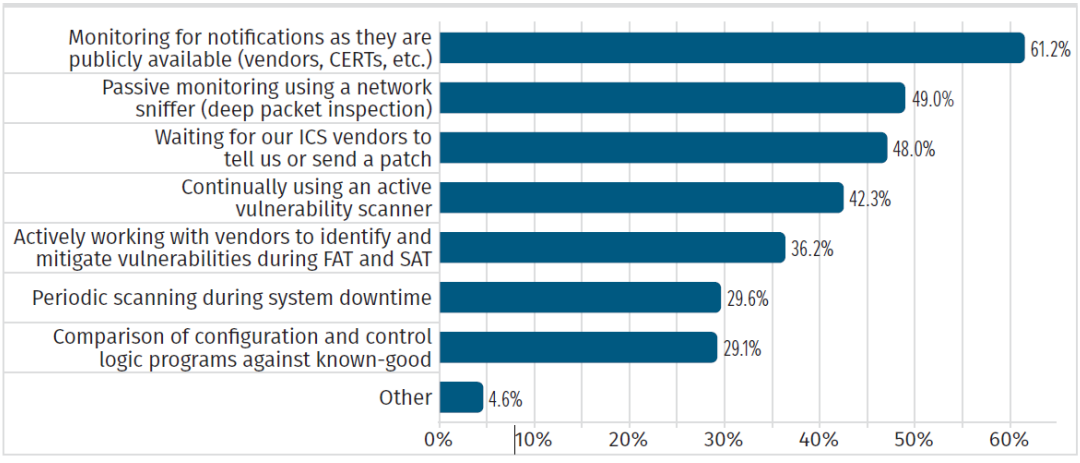

Figure 5 Processes are you using to detect software from SANS 2021 Survey: OT/ICS Cybersecurity

V dalším zkoumání pak byly řešeny další směry zvyšování bezpečnosti ICS systémů, které provozují. Jako největší technologické výzvy byly respondenty průzkumu vnímány tyto oblasti:

1) Technologicko-technická integrace – jak zajistit, aby účinnější integraci starších OT prostředí s moderními bezpečnostními technologiemi.
2) Nedostatek kvalifikovaných lidí a investic do jejich systematického rozvoje – a to na různých úrovních formálního i neformálního vzdělávání, profesního rozvoje, či rekvalifikací
3) Nastavení vhodných procesů a integrace mezi IT a OT/ICS prostředím tak aby odráželo doporučení dobré praxe kladené na Enterprise architekturu podniku.
4) Směřování k threat-hunting and detekci anomálií u OT systémů
5) Zaměření na adopci OT SOC a systémů rychlé detekce a reakce
6) Zvýšené využívání antimalwarových/antivirových řešení v OT prostředí

Způsoby zavedení systému řízení ICS

Existuje celá řada způsobů, jak danou problematiku uchopit. Pokud však organizace nemá odpovídající zkušenosti s implementací výše zmíněných frameworků, je vhodné začít s minimálním základem a postupně systém vylepšovat metodou jednotlivých cyklů PDCA. Metoda která by se dala popsat jako kroky idea-test-hodnocení, jinými slovy naplánuj-proveď-ověř-vylepši je znázorněná na obr6. na kterém je naznačen i obsah jednotlivých kroků.

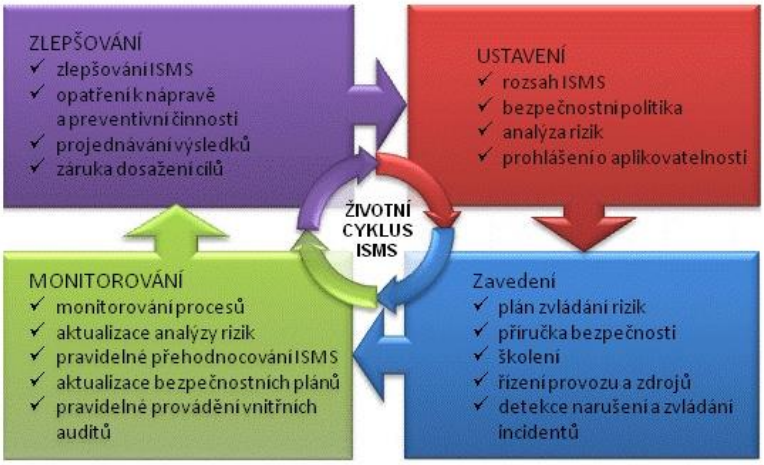

Figure 6 PDCA cyklus

Při jednotlivých krocích implementace je rovněž třeba vzájemně vyvážit i jednotlivé oblasti v systému řízení kybernetické bezpečnosti a to konkrétně oblasti:

1) Technického zajištění a nastavení
2) Nastavení odpovídajících procesů
3) Zajištění vyškolení jak koncových uživatelů, tak i zaměstnanců spravující OT/ICS systémy v odpovídající znalosti 1 a2

Jako vhodný přístup při zavádění z nuly lze zvolit v prostředí ČR doporučení Minimální bezpečnostní standard – podpůrný materiál pro subjekty, které nespadají pod zákon o kybernetické bezpečnosti[6] který vydala Národní komunikační agentura NAKIT ve spolupráci s Národním úřadem pro kybernetickou bezpečnost. Tento materiál je rozdělen na část:

1) Manažerskou, která se věnuje doporučení v oblastech
    a. Plánování zavádění bezpečnostních opatření
    b. Klasifikaci a ochraně informací
    c. Požadavků na řízení dodavatelů
    d. Řízení lidských zdrojů
    e. Řízení změn
    f. Řízení kontinuity činností
    g. Auditování kybernetické bezpečnosti
2) Technická část pak věnuje požadavkům na:
    a. Fyzickou bezpečnost
    b. Řízení přístupů
    c. Požadavky na ochranu před škodlivým kódem
    d. Otázce zvládání Kybernetických bezpečnostních události a incidentů
    e. Aplikační bezpečnosti
    f. Kryptografických prostředků
    g. Zajištění vysoké dostupnosti systémů
    h. A požadavkům v oblasti cloudových služeb.

Materiál pak ještě doplňuje přílohová část s přehledem politik, které by měli postupem času vzniknout, požadavky na dokumentaci celého systému a vzorový příklad plánu kontinuity činností. Vhodným doplňkovým materiálem pro začínající s implementací je rovněž Výkladový slovník kybernetické bezpečnosti[7]

Pro konkrétní minimální implementaci pak lze doporučit dokumenty Bezpečnostní doporučení NUKIB pro administrátory[8] ,Bezpečná práce na dálku[9].

Při praktické implementaci systému vzdělávání v oblasti informační bezpečnosti můžeme vycházet z doporučení NIST SP 800-16 [10], které definuje tzv. „vzdělávací kontinuum“ (Learning Continuum) pro jednotlivé role, které zaměstnanci zastávají v rámci organizace. Je zřejmé, že aby mohli zaměstnanci úspěšně plnit své role v rámci organizace, musí mít k dispozici správné nástroje a výcvik. Tzn. mimo nástrojů používaných ke své práci i vhodnou kombinaci bezpečnostního povědomí (security awareness), dovedností, praktických znalostí a schopností, které jsou pro každou roli potřebné

[6] Dostupné na https://archi.gov.cz/_media/dokumenty:2020-07-17_minimalni-bezpecnostni-standard_v1.0.pdf
[7] Petr JIRÁSEK, Luděk NOVÁK a Josef POŽÁR. Výkladový slovník kybernetické bezpečnosti. 3., doplněné a upravené vydání. vyd. Praha: Policejní akademie ČR v Praze, 2015. ISBN 978-80-7251-436-6.
[8] BEZPEČNOSTNÍ DOPORUČENÍ NÚKIB PRO ADMINISTRÁTORY 4.0 dostupné na https://www.nukib.cz/download/publikace/doporuceni/Doporuceni_admin_4.0_brozura_cb.pdf
[9] Bezpečná práce na dálku - doporučení pro firmy i zaměstnance https://www.nukib.cz/cs/infoservis/doporuceni/1523-bezpecna-prace-na-dalku-doporuceni-pro-firmy-i-zamestnance/
[10] NIST, Information technology security training requirements: A Role -Based Model for Federal Information Technology/Cybersecurity Training SP 800-16, USA [online]. [cit. 1. 1. 2019]. Dostupné z: https://csrc.nist.gov/CSRC/media/Publications/sp/800-16/rev-1/draft/documents/sp800_16_rev1_3rd-draft.pdf

Model na Obr7 ukazuje vhodnost jednotlivých úrovní vzdělávání pro vybrané kategorie:

- Úroveň "Security awareness" doporučení NIST výslovně vyžaduje pro všechny zaměstnance v rámci organizace.
- "Cybersecurity Essentials" je zapotřebí pro ty zaměstnance, včetně zaměstnanců dodavatelů, kteří jakýmkoli způsobem interagují s informačními systémy. Tento typ vzdělávání poskytuje základy k zvládnutí důležitých bezpečnostních termínů, pojmů a principů atp.
- „Role Based Training“ se zaměřuje na osvojení si specifických znalostí a dovedností, které zaměstnanec potřebuje, v rámci své role, k výkonu své činnosti. Na této úrovni vzdělávání respektuje rovněž rozdíly mezi kompetencemi kladenými na jednotlivé účastníky.
- Nejvyšší úroveň „Education" se pak zaměřuje na rozvoj schopností pracovat v multidisciplinárním prostředí, řešit problémy v týmové spolupráci a prohlubování dovedností ve své specializaci. Na tuto úroveň jsou pak zaměřeny dlouhodobé vzdělávací programy či mezinárodně uznávané certifikace.

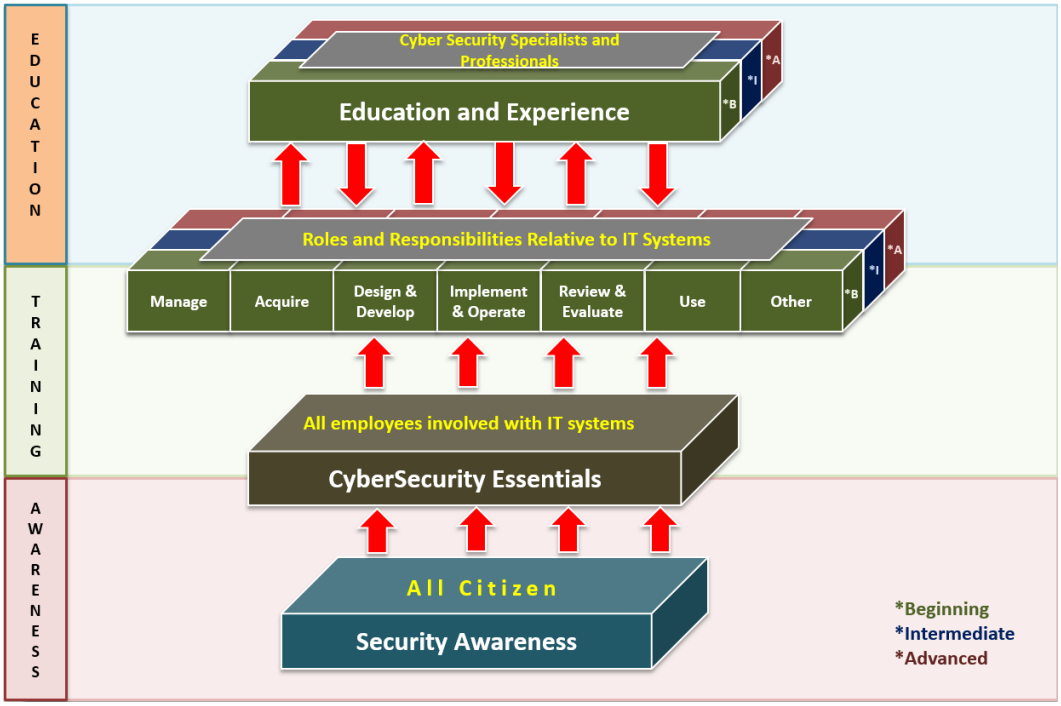

Figure 7 Cybersecurity Learning Continuum dle NIST[11]

[11] ZAHRI YUNOS, People factors in cyber resilience: creating the need for cybersecurity experts, [online]. [cit. 1. 1. 2022]. Dostupné z: https://slideplayer.com/slide/13731024/

Závěrem

Pro organizace, které již mají zkušenosti s procesním nastavením či implementací řízení bezpečnosti informací je pak vhodné využít řady norem IEC 62443, případně NIST SP 800-82 „Guide to Industrial Control Systems (ICS) Security. Zejména pak řada norem IEC 62443 obsahuje celou sadu doporučení pro řízení kybernetické bezpečnosti systémů ICS obdobně jako pro systémy IT řada norem ISO 270xx. Pro přehlednost zde jmenujme alespoň základní doumenty IEC 62443:

- IEC TS 62443-1-1:2009 - Průmyslové komunikační sítě – Bezpečnost sítí a systémů - Část 1-1: Terminologie, pojmy a modely
- IEC 62443-2-1:2010 - Průmyslové komunikační sítě – Bezpečnost sítí a systémů – Část 2-1: Zavedení programu bezpečnosti průmyslové automatizace a řídicích systémů
- EC TR 62443-2-3:2015 - Bezpečnost průmyslových automatizačních a řídicích systémů – Část 2-3: Správa záplat v prostředí IACS
- IEC 62443-2-4:2015+AMD1:2017 – Bezpečnost průmyslových automatizačních a řídicích systémů – Část 2-4: Požadavky na bezpečnostní program pro poskytovatele služeb IACS
- IEC TR 62443-3-1:2009 Průmyslové komunikační sítě – Bezpečnost sítí a systémů – Část 3-1: Bezpečnostní technologie pro průmyslové automatizační a řídicí systémy
- IEC 62443-3-2:2020 - Bezpečnost průmyslových automatizačních a řídicích systémů – Část 3-2: Posouzení bezpečnostních rizik pro návrh systému
- IEC 62443-3-3:2013 - Průmyslové komunikační sítě – Bezpečnost sítí a systémů – Část 3-3: Požadavky na bezpečnost systému a úrovně bezpečnosti
- IEC 62443-4-1:2018 - Bezpečnost průmyslových automatizačních a řídicích systémů – Část 4-1: Požadavky na bezpečný životní cyklus vývoje produktu
- IEC 62443-4-2:2019 - Bezpečnost průmyslových automatizačních a řídicích systémů – Část 4-2: Technické bezpečnostní požadavky na komponenty ICS